

In re Appln. of Bishop, et al.
App. No. 10/821,379

RECEIVED
CENTRAL FAX CENTER

NOV 06 2006

CLAIMS

Please amend the claims as follows:

Claims 1-4 (canceled).

Claim 5 (currently amended) A method for protecting a network server from being used as the basis of an attack on a network client, the method comprising:

- a. restricting access to said network server to a portion of said network server for at least a selected protocol; ~~[[and]]~~
- b. scanning said portion of said network server for particular characters, said particular characters being associated with said selected protocol; and, [[.]]
- c. removing said particular characters such that the security risk posed by said selected character is reduced.

Claim 6 (canceled)

Claim 7 (original) The method of Claim 5, further comprising replacing said particular characters with benign characters such that a security risk posed by said selected protocol is reduced.

Claim 8 (original) The method of Claim 5, wherein said characters are hostile characters and wherein if a request contains any of said hostile characters, the request is rejected.

Claim 9 (original) The method of Claim 5, further comprising logging said particular characters to form a security log.

Claim 10 (original) The method of Claim 9, further comprising reviewing said security log to determine whether said particular characters are hostile.

Claim 11 (original) The method of Claim 5, wherein said protection of the network server is accomplished during an electronic purchase transaction.

In re Appln. of Bishop, et al.
App. No. 10/821,379

Claim 12 (original) The method of Claim 11, wherein the electronic purchase transaction is conducted using a digital wallet.

Claims 13-42 (cancelled).

Claim 43 (currently amended) A computer-implemented method for protecting a network server from being used as the basis of an attack on a network client, the method comprising:

- a. receiving a request for a connection at said server from said network client;
- b. scanning a portion of said network server for particular characters associated with a protocol;
- c. removing said particular characters such that the security risk posed by said selected character is reduced;
- [[c.]] d. verifying that any response from said network server to said network client is void of said particular characters; and
- [[d.]] e. providing said response from said network server to said network client.

Claim 44 (previously presented) The method of Claim 43 further comprising restricting access to said network server for said protocol to said portion of said network server.

Claim 45 (previously presented) The method of Claim 43 further comprising replacing said particular characters with benign characters such that a security risk posed by said selected protocol is reduced.

Claim 46 (previously presented) The method of Claim 43 wherein said protocol comprises javascript.

Claim 47 (previously presented) The method of Claim 43 further comprising logging said particular characters to form a security log.

In re Appln. of Bishop, et al.
App. No. 10/821,379

Claim 48 (previously presented) The method of Claim 47 further comprising reviewing said security log to determine whether said particular characters are hostile.

Claim 49 (previously presented) The method of Claim 47 wherein said protection of the network server is accomplished during an electronic purchase transaction.

Claim 50 (previously presented) The method of Claim 49 wherein the electronic purchase transaction is conducted using a digital wallet.